International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Intelligent Security Threat Detection in Cloud Computing Using Machine Learning Techniques

Dr. Nilesh Jain
Associate Professor
Department of Computer Science and Applications
Mandsaur University, Mandsaur, India
nileshjainmca@gmail.com

***Abstract*—Cloud computing has now become a basic platform of scalable data storage and distributed services, but its dynamic and multi-tenant nature exposes it to advanced cybersecurity risks. Traditional security measures, in most cases, do not detect evolving and zero-day attacks in real time. The proposed study aims to develop a machine learning (ML)-based threat detection system to improve intrusion detection in cloud environments using the NSL-KDD dataset. The methodology involves preprocessing, feature selection based on Random Forest and gradient boosting, XGBoost, and a stacked ensemble of Decision Tree, RF, and gradient boosting, using logistic regression as a meta-learner. The accuracy, precision, recall, F1score, and AUC-ROC are used to evaluate the performance. The results of the experiment indicate strong detection performance, with up to 99% accuracy and an AUC of 1.0, which is excellent for classification. The suggested solution enhances detection reliability, minimizes misclassification, and offers a scalable, data-driven approach to strengthen cloud security infrastructures.**

Keywords*—Cloud Computing Security, Machine Learning, Cyber Threat Detection, Cloud Network Security, Predictive Analytics.

I. INTRODUCTION

Software, networking, and data storage have all been revolutionized by cloud computing. They are hosted on remote servers and accessed online [1][2]. This technology offers scalability, cost efficiency and accessibility, making it a popular choice for businesses and individuals [3][4][5]. While it offers many benefits, it also presents challenges, especially around security, and the Cybersecurity industry plays a crucial role in identifying and implementing solutions. Cloud is vulnerable to Malware, Viruses, Phishing, SQL injection, Cross-Site scripting, DoS Attack, Zero-Day, man-in-the-middle attacks, and many more [6][7][8][9], are used by cyber criminals to steal data and disrupt services to prevent such attacks Intrusion Detection and anomaly-based detection play a crucial role, and as the advisories get smarter, the Cybersecurity industry needs to keep pace in inventing better methods and security solutions to counter cybersecurity attacks [10][11]. The dependability of services offered in different industries is greatly jeopardized by these dangers, which also endanger data integrity and privacy [12][13]. Therefore, it is crucial to improve security measures in cloud systems[14][15][16][17]. Traditional security measures, which frequently have static rule-based systems in place, are becoming less and less effective against the increasingly sophisticated cyberattacks that are emerging at a rapid rate [18]. They not only need a lot of resources, but they are also incapable of adapting to novel threats. As a result, there has been a significant movement in cybersecurity toward the application of artificial intelligence (AI) [19][20]. With its ability to learn from received data, AI-powered systems offer a dynamic security solution that is presented in [21][22]. ML is a form of AI that enhances the detection of threats by enabling the computer to learn from previous data, find complex patterns and adapt to new attack methods [23][24][25]. These models can estimate potential vulnerabilities, detect subtle behavioral changes, and provide real-time alerts. Supervised learning, unsupervised anomaly detection, and clustering are common methods used to identify dangers that might otherwise go unnoticed [26][27]. ML is highly effective in improving the overall security posture by improving the accuracy of detection, reducing false positives, and supporting automated incident triage [28][29]. Large volumes of data may be processed and analyzed in real time by AI and ML algorithms, which can detect abnormalities and new threats far more quickly and accurately than traditional techniques [30][31]. Large volumes of security-related data may be processed by AI and ML to find trends and abnormalities that could point to a danger.

A. Motivation and Contributions of the Study

The rapid rate of cloud computing adoption across industries has posed complex security issues as a result of shared resources, virtualized infrastructures, and constantly changing cyber threats. Conventional rule-based intrusion detection systems generate many false alerts because they cannot adapt to new attack patterns. This is what makes it necessary to have intelligent, automated threat detection mechanisms that are able to learn based on large-scale network data. ML can detect concealed attack behaviors, enabling proactive and precise protection for the modern cloud ecosystem. The major contributions of the study are given:

- Proposes a ML-based approach for identifying cybersecurity risks in cloud environments.
- Implements comprehensive preprocessing, including encoding, normalization, and class balancing, to improve data quality.
- Reduces dimensionality and improves computing performance by using RF-based feature selection.
- Develops a stacked ensemble model and XGBoost to compare robustness and predictive performance.
- Provides a flexible and scalable solution appropriate for monitoring cloud security in real time.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

B. Justification and Novelty of the paper

The research is supported by the increasing need of lightweight, precise and scalable threat detection solutions, specific to cloud environments. In contrast to the current literature, where the studies focus on single-model-based identification, or the one-dimensional detection schemes, the proposed work suggests a hybrid ensemble framework, which combines feature-optimized learning with stacked generalization and XGBoost. The novelty is that it combines the capabilities of Feature selection based on the Random Forest algorithm and ensemble intelligence to increase both detection accuracy and reduce false prediction and improve generalization to a variety of cloud traffic patterns.

C. Structure of the paper

The following is the paper's structure: In Section II, research gaps are noted and relevant literature is explored. Section III goes into depth on the model's development technique and process. Section IV provides specifics on the results of the studies and comparisons. Section V ends the study and sets out the priorities for future research.

II. Literature of Review

Recent studies highlight ML and DL methods to identify cloud security threats and pay attention to accuracy, anomaly detection, scalability, and real-time monitoring in environments.

A. K. Shukla et al. (2026) introduce the Shuffle Attention Convolutional Forward Fractional Network (SACFFNet) to overcome the flaws in cloud computing by identifying performance-compromising attacks. Shuffle Attention Networks and Convolutional Neural Networks are modified to use Fractional Calculus and SACFFNet has a performance of 91.678% acc, 92.884% sensitivity and 92.090% specificity [32]. X. Jiang et al. (2025) showcase a DL model that utilises LSTM analysis and attention to discover anomalies and early warning systems of threats in cloud-based infrastructures in real-time. The system has a prec of 94.2, a rec of 95.7, an accuracy of 96.8 and an average lead time of 142 with the threat prediction. Its application in three large cloud systems proves its scalability and its efficiency of work in the enterprise products [33].

V. Mamidala et al. (2025) conducted a study to evaluate efficacy of the Isolation Forest (iForest) algorithm in detecting anomalies in cloud environments to protect data and information from cyber threats. The iForest algorithm was more successful than traditional methods, scoring an average of 0.842 and a FNR of 0.06, at a fast processing time. The findings show that iForest can simply be integrated with the current security infrastructures and greatly increase threat detection accuracy [34]. T. A. Devi and A. Jain (2024) presented a novel DL-based method for cloud computing intrusion detection. They emphasize the need to supplement training data to increase the detection effectiveness of offline and online training. Soft-max regression and STL are capable of learning features that result in a higher than 98% accuracy in various classification categories [35].

D. Chaudhary et al. (2024) suggests a cutting-edge AI-based strategy to improve cloud-based cyber threat identification and mitigation. The suggested approach attains 98.5% detection acc as opposed to the current system's 89.7%, while lowering the FN and FP rates to 2.0% and 1.2%, respectively [36]. P. Parameswarappa et al. (2023) provide a novel firewall approach that uses a ML algorithm to ensure cloud computing is secure. By merging previous node judgements with the ML algorithm's output on the publicly accessible UNSW-NB-15dataset, the suggested approaches predict the final attack category and enhance anomaly detection by 97.68% [37].

A. Critical Gaps in Existing Research

Although there have been significant improvements regarding ML-based security measures to cloud computing, a number of constraints remain. The existing methods are mostly focused on high detection rates but do not consider real-time flexibility against existing and zero-day attacks in dynamic cloud environments. Also, most models are based on static or benchmark datasets that fail to reflect complexity of multi-tenant, large-scale cloud infrastructures, which prevents real-world usage. Computational cost, scalability, and resource-constrained cloud systems integration are issues that have not been sufficiently studied. Further, explainable, and lightweight frameworks, which may be able to guarantee efficient threat detection whilst at the same time preserving privacy, interoperability and ensuring continuous learning in heterogeneous cloud ecosystems, cannot be explained.

III. Methodology

The proposed algorithmic solution to the problem of cloud security threat detection using machine learning (Fig. 1) begins with the data collection based on NSL-KDD dataset, and consists of intrusion logs and network traffic. Preprocessing of the raw data is performed, which includes data cleaning, one-hot encoding, normalization with the help of a standard scaler, and balancing with the help of a Random Over Sampler to address class imbalance. The most relevant characteristics are then found by feature selection utilizing an RF technique, increasing model efficiency. Training (80%) and testing (20%) subsets are created from the processed data. It suggests a combination of DT, RF, and GB or XGBoost as a threat detection model. To provide proper identification, studies use such measures as F1score, acc, prec, rec, and AUC-ROC to assess performance of models.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

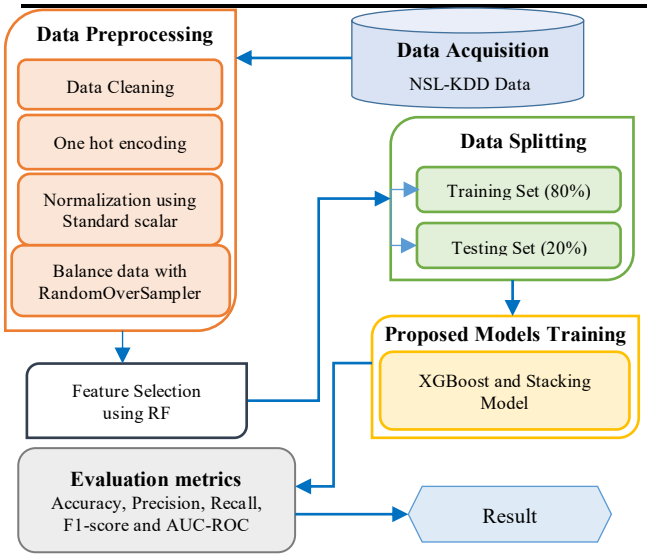

Fig. 1. Workflow of Machine Learning–Based Threat Detection in Cloud Networks.

A. Data Collection

This study makes use of the NSL-KDD dataset, which is an improved version of the KDD Cup'99 dataset that was created to get over issues with duplication and class imbalance. It comprises 41 characteristics such as categorical, binary, and continuous variables that manifest different network traffic patterns. Additionally, the instances are divided into regular and attack categories, with DoS, Probe, R2L, and U2R being the attack types. Due to its enhanced data distribution and less bias, NSL-KDD is highly apt in benchmarking intrusion detection system in cloud and network security studies.

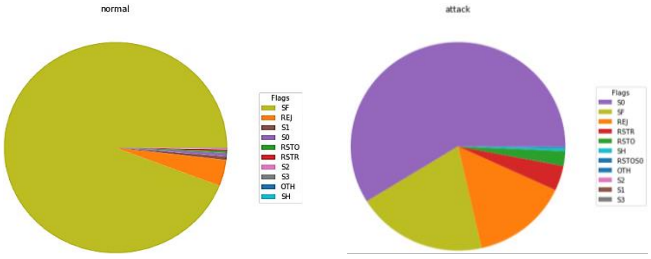

Fig. 2. Distribution of Connection Flags in Normal and Attack Network Traffic.

Fig. 2 provides the comparison between connection flag distributions of normal and attack traffic. Normal traffic is predominantly comprised of the SF flag, which is a successful connection, whereas the attack traffic includes a broader variety of flags including S0, REJ, and RSTR, which are an abnormal or failed connection attempt.

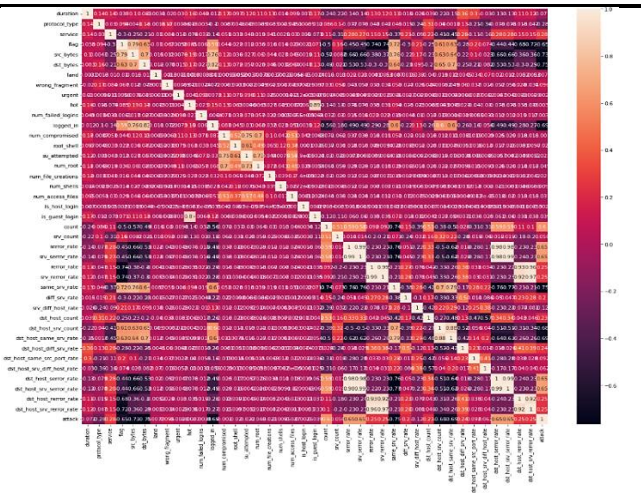

Fig. 3. Correlation Matrix of Network Traffic Features.

A heatmap of the Correlation Matrix for the network traffic characteristics is shown in Fig. 3, with color intensity denoting the strength and direction of correlations between variables. Light colors denote positive correlations, whereas the dark colors present weak or negative associations.

B. Data Preprocessing

Data pre-processing is crucial to prepare data to be selected according to features because machine learning algorithms need numerical and clean data. The following steps are undertaken to achieve this:

1) Data Cleaning

Data cleaning is done to ensure the correctness and uniformity of the dataset prior to modelling training. The data are analyzed in terms of duplicate entries, null records, and formatting errors. The extra spaces and other unusual characters are then eliminated from the categorical data that has been categorized as protocol type, service, and flag. The step removes noise and provides reliable and structured data to model intrusion detection accurately.

2) Encoding

Encoding is carried out to encode categorical attributes in the data to numerical representations that can be processed with machine learning algorithms. The protocol type and service, as well as flag features, are coded as one-hot features. This guarantees that the category information is maintained without violation of ordinal bias. The encoded data allows the classifiers to do processing on network traffic characteristics to make intrusion determination.

3) Normalization

The pre-processing method in ML is that the dataset features were normalized to a mean of 0 and a standard deviation of 1 using the Standard Scaler [38]. The average and standard deviation for every feature in the dataset are computed as in Equation (1):

$$z = \frac{x-\mu}{\sigma} \quad (1)$$

Where z represents a normalised value, x is the original feature value, μ denotes the mean of the feature, and σ denotes its Standard Deviation.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

4) Balance data with Random Over Sampler

Random Over Sampler to increase the number of instances of minority classes is used to counteract the disparity between the NSL-KDD dataset's classifications. The class distribution of the data before and after balancing is shown in Fig. 4. Firstly, the data was skewed (67,343 normal and 58,630 attack), though, with the oversampling, the data were equalized (67,343 samples per classes), therefore, making both balanced when training the model.

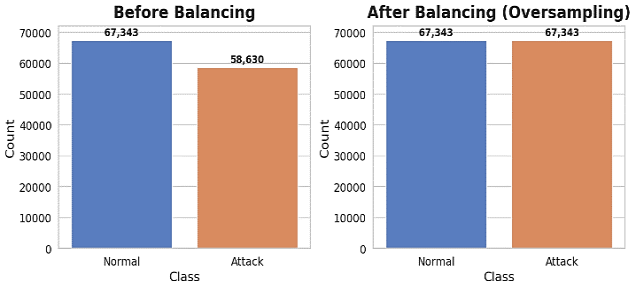

Fig. 4. Data Distribution Before vs After Balancing.

5) Feature Selection using RF

Random Forest feature selection identifies the most important attributes using feature importance scores, which are based on decision tree splits. Key selected features include **src_bytes, data_transfer, same_srv_rate, count, dst_bytes, dst_host_serror_rate, dst_host_diff_srv_rate, dst_host_srv_serror_rate, srv_serror_rate, error_rate, and attack.** The more important features are retained, and less significant ones are eliminated, resulting in dimensionality reduction and enhancing the model's effectiveness and generalization.

6) Data Splitting

In this analysis, each dataset is split into two parts at an 80:20 ratio. The majority, 80%, is used to train the model, with the remaining 20% reserved for performance assessment.

C. Implementation of ML Models

The proposed models are defined below, which are used for prediction the cloud security [39].

1) Stacking Model

The proposed method involves the stacking of ensemble model, which combines DT, RF, and GB as base learners to improve classification strength and predictive power [40][41]. The bottom level of the stacked architecture has individual base classifiers that are trained separately on the training data and thus are able to extract a variety of decision patterns and interactions between features. K-fold cross-validation is utilized to obtain out-of-fold prediction using each of the base models in order to obtain reliable performance and to reduce over-fitting.

These initial-level predictions are then put together to create a new space of features which are fed into a second-level meta-learner on LR. LR is a linear probabilistic classifier which is based on a sigmoid activation function in order to estimate the probability of a class and models the relation between the input variables and the target class. LR as a meta-learner determines the best weightings of the prediction of DT, RF, and GB, which is the degree of influence that each base model is supposed to contribute to the final decision. The strategy can be further enhanced by layering the models to achieve complementary strengths, reduce bias, and variance and enhance their overall generalization behavior over individual classifiers.

2) XGBoost Model

The decision trees of XGBoost, a better ensemble learning method based on gradient boosting, are constructed upon one another, and each subsequent tree is intended to eliminate the errors made by other trees [42]. XGBoost enhance the capability of classification in the proposed intrusion detection model, by taking into account the complicated nonlinear relationship amid network traffic characteristics. Its residual-learning algorithm allows self-improvement allowing it to operate its accurate detection of normal and malicious processes which increases its detection accuracy and strength. The XGBoost problem is defined as illustrated in Equation (2).

$$\mathcal{L}(\emptyset) = \sum_{i=1}^{n} l(y_i, \hat{y}_i) + \sum_{k=1}^{K} \Omega(f_k) \quad (2)$$

Where $\mathcal{L}(\emptyset)$ represent the overall loss function, l is a differentiable convex loss function that measures discrepancy among the forecast results $\hat{y}_i$ and the true value y_i , and Ω is the phrase used for regularization, which reduces the model's complexity.

In training it is a gradient-based optimization of this objective function, which is reduced by the model with hyperparameters including Learning Rate, tree depth, and number of estimators being optimized to obtain the best possible generalization performance.

D. Evaluation Metrics

The effectiveness of the proposed plan can be measured using the indicators provided in this section. TP, TN, FP, and FN were the fundamental elements of the evaluation [43]. Accuracy, or the proportion of accurate forecasts to all instances, is one of the primary performance metrics based on these figures. Precision is used to determine the accuracy of optimistic forecasts. Recall gauges how well the model can find all pertinent examples. F1score particularly, can be used where there is imbalance in the classes since it considers both FP and FN. In order to depict the sensitivity and the FPR at different thresholds it make the ROC curve. A greater number approaching 1 indicates strong performance when measuring the AUC, which is utilized to quantify the overall performance of the model. The Mathematical computation is shown in Equations (3) to (7).

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (3)$$

$$Precision = \frac{TP}{TP+FP} \quad (4)$$

$$Recall = \frac{TP}{TP+FN} \quad (5)$$

$$F1 = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (6)$$

$$AUC = \int_0^1 TPR(FPR)d(FPR) \quad (7)$$

Where FPR stands for false positive rate and TPR for true positive rate. This comprehensive assessment of the models' efficacy is achieved when these metrics are combined.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

IV. Result Analysis and Discussion

The experiments were performed within the Windows-based system that provided a high-performance AMD Ryzen 9 processor and 64 GB RAM to provide efficient training and evaluation of various models. The two suggested methods, Stacking and XGBoost, for identifying security risks in cloud computing settings are compared in Table I. Both models are highly predictive, virtually perfect on all evaluation criteria. Although both models achieve an AUC-ROC of 1.0, demonstrating outstanding classification effectiveness and reliability, the stacking model notably outperforms XGBoost in acc, prec, rec and F1score.

TABLE I. Performance Analysis of Proposed Ensemble Stacking and XGBoost Model

Metric	Stacking model	XGBoost model
Accuracy	99.0	98.79
Precision	99.2	98.78
Recall	99.7	99
F1-Score	99.45	98.89
AUC-ROC	1.0	1.0

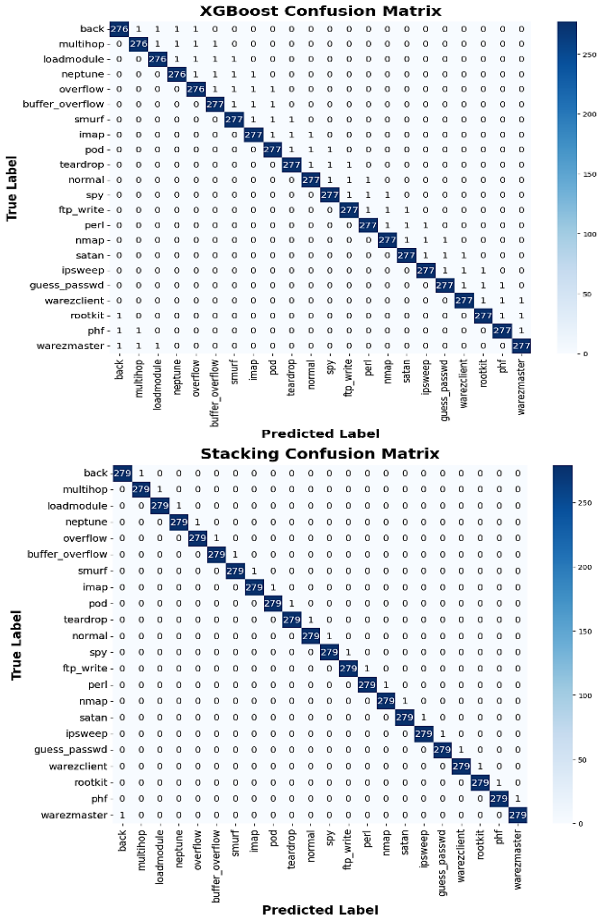

Fig. 5. Confusion Matrix of XGBoost Model for threat detection in the cloud.

The confusion matrices in Fig. 5 indicate that both the XGBoost and stacking ensemble model possess very high classification accuracy on 22 attack types and the normal category. The diagonal values (almost 276–279 accurate forecasts for each class) are strong and almost zero-off-diagonal values show that there is little misclassification. This demonstrates the high accuracy of the models and their potential to successfully discriminate between various cyber threats.

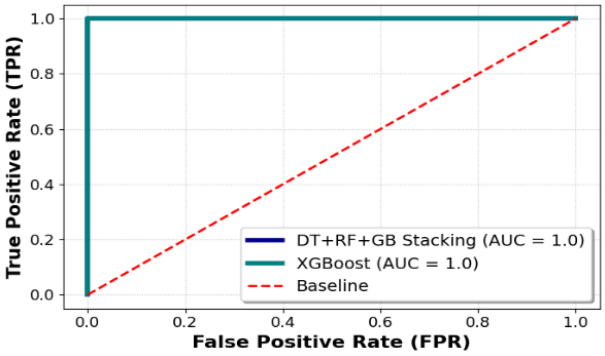

Fig. 6. ROC Curve of Stacking Ensemble and XGBoost Models.

The ROC curve in Fig. 6 indicates that both the XGBoost and Stacking Ensemble models perform exceptionally well, with an AUC of 1.0. This implies that it is perfectly classified with a 100 percent true positive rate and zero false positives, which points to their efficiency in identifying various cybersecurity threats.

A. Comparative Analysis

Table II displays the results of comparing several ML models implemented on various intrusion detection datasets. The model with the highest performance is the proposed one based on the NSL-KDD dataset, the accuracy of the Stacking model is 99.0 percent, XGBoost is 98.79 percent, which is higher than past-reported models. Other works present lower accuracies, such as RF-RBFNN (94.16%) on NSL-KDD, KNN (98.21%) on SDN Data, ANN (92.0%) on ISOT-CID, and SVM (94.32%) on CICDDoS2019. In general, the results indicate that the ensemble-based method proposed achieves better detection rates than current methods.

TABLE II. Comparative Performance Analysis of Machine Learning Models for Cloud Security

Reference	Dataset	Models	Accuracy
Proposed	NSL-KDD	Stacking model	99.0
Proposed	NSL-KDD	XGBoost	98.79
[44]	NSL-KDD	RF-RBFNN	94.16
[45]	SDN Data	KNN	98.21
[46]	ISOT-CID	ANN	92.0
[47]	CICDDoS2019	SVM	94.32

B. Discussion

The experimental results indicate that when the ability of numerous classifiers is combined, ensemble learning significantly enhances cloud-based cybersecurity threats detection. The stacking model, especially, demonstrated better performance because it is capable of incorporating different decision patterns and decreasing both bias and variance. The large AUC-ROC and low misclassification rates show great generalization ability to differentiate normal and malicious traffic. The proposed framework is more accurate than the current methods and offers better computational efficiency as a result of feature selection. Nevertheless, the controlled dataset environment might fail to capture dynamic attack patterns, and it is important to emphasize that real-time

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

validation, as well as adaptive learning mechanisms, should be deployed in dynamic cloud infrastructure.

V. Conclusion and Future Work

An ML-based system was developed to detect cybersecurity problems in cloud computing environments with advanced ensemble learning approaches. By combining extensive preprocessing, feature selection using the Random Forest algorithm, and having such a powerful classifier as XGBoost and a stacked ensemble model, the system was able to identify malicious activities with a high accuracy and reliability. The stacking model was better in all the measures of evaluation, showing the effectiveness of using a combination of multiple learners to learn the tricky and dynamic attack patterns. The findings highlight the fact that highly intelligent data-driven detection mechanisms can go a long way in outshining the traditional intrusion detection methods in terms of improving the detection of anomalies and reducing false alarms. The suggested architecture can be widely applied in the current distributed cloud infrastructures due to its scalability and flexibility. Although the results were encouraging, this test was mainly performed on benchmark collections, and this may not be the dynamic and heterogeneous nature of actual cloud environments. Future studies will focus on validation on live cloud traffic and large-scale, multi-tenant systems so that it can be practically applicable. The transparency, interpretability, and user confidence in automated threat detection systems will also increase due to the explainable artificial intelligence methods that will be used. In addition, exploring lightweight and federated learning solutions will be useful in conducting privacy-conscious, real-time monitoring with less computational requirements that will enable to carry out threat detection in a safe and efficient way under the different and resource-constrained cloud computing environments.

References

[1] K. K. Mohammed, "The Future is Cloud: Modernizing Big Data for the Cloud Era," *Int. J. Sci. Res. Eng. Trends*, vol. 11, no. 5, pp. 1–5, 2025.

[2] S. B. Karri, C. M. Penugonda, S. Karanam, M. Tajammul, S. Rayankula, and P. Vankadara, "Enhancing Cloud-Native Applications: A Comparative Study of Java-To-Go Micro Services Migration," *Int. Trans. Electr. Eng. Comput. Sci.*, vol. 4, no. 1, pp. 1–12, Apr. 2025, doi: 10.62760/iteecs.4.1.2025.127.

[3] S. Singamsetty, "An Intelligent Framework for Secure and Fair Cloud Resource Distribution," in *2025 7th International Conference on Innovative Data Communication Technologies and Application (ICIDCA)*, IEEE, Oct. 2025, pp. 686–690. doi: 10.1109/ICIDCA66325.2025.11280502.

[4] A. Warrier, "Securing and Scaling API Gateways in Hybrid Environments," *J. Artif. Intell. Mach. Learn. Data Sci.*, vol. 3, no. 3, pp. 2914–2920, Sep. 2025, doi: 10.51219/JAIMLD/Arjun-warrier/607.

[5] M. Parikh, A. A. Soni, S. M. Shah, and A. R. Jha, "Big Data Workload Profiling for Energy-Aware Cloud Resource Management." 2026. doi: 10.48550/arXiv.2601.11935.

[6] B. Singh, H. Singh, and T. Banerjee, "Strengthening Modern IAM Authentication with Quantum Cryptography and Anti-Phishing Techniques," *Sarcouncil J. Eng. Comput. Sci.*, vol. 4, no. 10, Oct. 2025, doi: 10.5281/zenodo.17260292.

[7] S. Singh, "Advancing Network Security in 5G: Leveraging the 5G-NIDD Dataset for Intrusion Detection and Mitigation," in *2025 IEEE 12th International Conference on Cyber Security and Cloud Computing (CSCloud)*, IEEE, Nov. 2025, pp. 1–6. doi: 10.1109/CSCloud66326.2025.00055.

[8] V. K. Sharma, "Cloud Computing IoT: 5G Focused IoT with Cloud Solutions," *Int. J. AI, BigData, Comput. Manag. Stud.*, vol. 6, no. 3, 2025, doi: 10.63282/3050-9416.IJAIBDCMS-V6I3P103.

[9] V. Varma, "Secure Cloud Computing with Machine Learning and Data Analytics for Business Optimization," *ESP J. Eng. Technol. Adv.*, vol. 4, no. 3, 2024, doi: 10.56472/25832646/JETA-V4I3P119.

[10] R. V. S. S. B. R, Y. M. M. John, M. B. B. G, B. Karim, and G. Saritha, "Multi-Domain Cyber Threat Classification Using Enhanced Genetic Algorithm and Deep Neural Networks," in *2025 Third International Conference on Networks, Multimedia and Information Technology (NMITCON)*, IEEE, Aug. 2025, pp. 1–6. doi: 10.1109/NMITCON65824.2025.11187556.

[11] J. E. Kofi, "Monitoring Cloud Performance Metrics Utilizing AI to Estimate the Efficiency of Cloud Operations," in *2025 7th International Symposium on Advanced Electrical and Communication Technologies (ISAECT)*, IEEE, Dec. 2025, pp. 1–6. doi: 10.1109/ISAECT68904.2025.11318827.

[12] S. Singamsetty, "CyNet: Amalgam Deep Learning Model for Multi-Vector Cyber Intrusion Detection System (IDS)," in *2025 3rd International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI)*, IEEE, Sep. 2025, pp. 914–918. doi: 10.1109/ICoICI65217.2025.11253990.

[13] G. Modalavalasa, "Analysis and Optimization of Privacy-Preserving Encryption Techniques in Cloud Computing Environments for Secure Cloud Data," in *2025 5th International Conference on Intelligent Technologies (CONIT)*, IEEE, Jun. 2025, pp. 1–6. doi: 10.1109/CONIT65521.2025.11167685.

[14] P. C. Jakku, P. Sundaramoorthy, S. C. Kondaparthy, T. Desai, R. Jarubula, and A. Nerella, "Enhancing Cloud Security Via Quantum Computing," in *Proceedings of Data Analytics and Management*, A. Swaroop, B. Virdee, S. Correia, and Z. Polkowski, Eds., Cham: Springer Nature Switzerland, 2026, pp. 377–386. doi: 10.1007/978-3-032-03558-5_31.

[15] R. Lingam, "Zero-Trust Architectures for Secure DevOps Automation in Enterprise AI Systems," *Milestone Trans. Artif. Intell.*, vol. 1, no. 1, pp. 18–33, 2026, doi: 10.5281/zenodo.18439428.

[16] A. Gupta, "What Is The Right Security Posture? A Perspective on Cloud Computing Security Threats and Risk Assessment," *Int. J. Emerg. Res. Eng. Technol.*, vol. 4, no. 4, 2023, doi: 10.63282/3050-922X.IJERET-V4I4P112.

[17] V. Shah, "Managing Security and Privacy in Cloud Frameworks: A Risk with Compliance Perspective for Enterprises," *Int. J. Curr. Eng. Technol.*, vol. 12, no. 06, pp. 1–13, 2022, doi: 10.14741/ijcet/v.12.6.16.

[18] A. Parupalli and H. Kali, "A Comprehensive Review of Cost Optimization Strategies in Multi-Cloud Environments," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 5, June, pp. 1043–1052, 2023, doi: 10.48175/IJARSCT-11937Q.

[19] R. rao Thallada and N. Alapati, "Privacy and Cybersecurity Convergence: GRC Controls for Data Protection," *J. Bus. Manag. Stud.*, vol. 8, no. 5, pp. 42–48, 2026.

[20] A. R. Bilipelli, "AI-Driven Intrusion Detection Systems for Large-Scale Cybersecurity Networks Data Analysis : A Comparative Study," *TIJER – Int. Res. J.*, vol. 11, no. 12, pp. 922–928, 2024.

[21] A. Katangoori, "The Role of Big Data in Advancing Artificial Intelligence: Methods and Case Studies," *Int. J. Artif. Intell. Mach. Learn.*, vol. 6, no. 1, pp. 37–54, Jan. 2026, doi: 10.51483/IJAIML.6.1.2026.37-54.

[22] A. R. Toorpu, S. K. Vududala, A. Nerella, and B. P. Madupati, "Hybrid AI Models for Privacy-Preserving Big Data Analytics in Distributed Environments," in *2025 Global Conference in Emerging Technology (GINOTECH)*, IEEE, May 2025, pp. 1–8. doi: 10.1109/GINOTECH63460.2025.11076666.

[23] V. K. Bollu, "Threat Landscape in Artificial Intelligence Systems: Taxonomy, Attack Vectors and Security Implications," *World J. Adv. Res. Rev.*, vol. 29, no. 1, pp. 285–294, 2026, doi: 10.30574/wjarr.2026.29.1.0007.

[24] S. K. Chintagunta and S. Amrale, "Enhancing Cloud Database Security Through Intelligent Threat Detection and Risk Mitigation," *TIJER*--

Int. Res. J, vol. 9, no. 10, pp. 49–55, 2022.

[25] S. K. Chintagunta, "Enhancing Cloud Database Security Through Intelligent Threat Detection and Risk Mitigation," *TIJER – Int. Res. J.*, vol. 9, no. 10, pp. 49–55, 2022.

[26] D. Bhattacharjee, "Design and Evaluation of Deep Generative AI Model for Intrusion Detection in Cyber Threat Monitoring," in *2025 7th International Symposium on Advanced Electrical and Communication Technologies (ISAECT)*, IEEE, Dec. 2025, pp. 1–6. doi: 10.1109/ISAECT68904.2025.11318752.

[27] G. Sarraf and V. Pal, "Autonomous Threat Detection and Response in Cloud Security: A Comprehensive Survey of AI-Driven Strategies," *Int. J. Emerg. Res. Eng. Technol.*, vol. 6, no. 4, 2025, doi: 10.63282/3050-922X.IJERET-V6I4P114.

[28] S. Thangavel, S. Srinivasan, S. B. V. Naga, and K. Narukulla, "Distributed Machine Learning for Big Data Analytics: Challenges, Architectures, and Optimizations," *Int. J. Artif. Intell. Data Sci. Mach. Learn.*, vol. 4, no. 3, pp. 18–30, Oct. 2023, doi: 10.63282/3050-9262.IJAIDSML-V4I3P103.

[29] P. Chandrashekar and M. Kari, "Design Machine Learning-Based Zero-Trust Intrusion Identification Models for Securing Cloud Computing System," *Int. J. Res. Anal. Rev.*, vol. 11, no. 4, pp. 901–907, 2024.

[30] D. Jain and S. Jain, "Artificial Intelligence (AI)-Driven Network Traffic Anomaly Detection for IT Infrastructure Security," in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, IEEE, Feb. 2026, pp. 1–6. doi: 10.1109/ICAIC67076.2026.11395685.

[31] S. Narang and A. Gogineni, "Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud Environment," *Int. J. Sci. Res. Mod. Technol.*, vol. 4, no. 5, pp. 60–70, Jun. 2025, doi: 10.38124/ijsrmt.v4i5.542.

[32] A. K. Shukla, A. Sharma, and S. S. Sengar, "SACFFNet : Shuffle Attention Convolutional Forward Fractional Network Based Attack Detection in Cloud Computing," *Concurr. Comput. Pract. Exp.*, vol. 38, no. 3, Feb. 2026, doi: 10.1002/cpe.70504.

[33] X. Jiang, R. Jia, and F. Zhang, "Deep Learning-Based User Behavior Anomaly Detection and Threat Early Warning in Cloud Computing Environments," *Acad. Nexus J.*, vol. 4, no. 3, pp. 1–24, 2025.

[34] V. Mamidala, A. R. G. Yallamelli, M. V. Devarajan, T. Ganesan, R. K. M. K. Yalla, and A. Sambas, "Hybrid anomaly-based cloud security and machine learning-based behavioral analysis for threat intelligence detection in cloud environment," *Cluster Comput.*, vol. 28, no. 8, p. 485, Sep. 2025, doi: 10.1007/s10586-024-05025-x.

[35] T. A. Devi and A. Jain, "Enhancing Cloud Security with Deep Learning-Based Intrusion Detection in Cloud Computing Environments," in *2024 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT)*, 2024, pp. 541–546. doi: 10.1109/InCACCT61598.2024.10551040.

[36] D. Chaudhary, S. K. Verma, V. M. Shrimal, R. Madala, R. Baliyan, and S. M, "AI-Based Methods to Detect and Counter Cyber Threats in Cloud Environments to Strengthen Cloud Security," in *2024 International Conference on Electrical Electronics and Computing Technologies (ICEECT)*, IEEE, Aug. 2024, pp. 1–6. doi: 10.1109/ICEECT61758.2024.10739173.

[37] P. Parameswarappa, T. Shah, and G. R. Lanke, "A Machine Learning-Based Approach for Anomaly Detection for Secure Cloud Computing Environments," in *2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, IEEE, Jan. 2023, pp. 931–940. doi: 10.1109/IDCIoT56793.2023.10053518.

[38] P. Nutalapati, J. R. Vummadi, S. Dodda, and N. Kamuni, "Advancing Network Intrusion Detection: A Comparative Study of Clustering and Classification on NSL-KDD Data," in *2025 International Conference on Data Science and Its Applications (ICoDSA)*, IEEE, Jul. 2025, pp. 880–885. doi: 10.1109/ICoDSA67155.2025.11157595.

[39] S. A. Pushkala, "Financial Fraud Identification Using Graph Neural Network And LSTM With Autoencoder-Based Data Refinement," *J. Int. Cris. RISK Commun. Res.*, vol. 9, no. 1, pp. 198–214, 2026.

[40] S. B. Shah, B. Boddu, N. Prajapati, and S. A. Pahune, "AI-Powered Advanced Intrusion Detection for Securing Cloud Environments Against Network Attacks," in *2025 Global Conference in Emerging Technology (GINOTECH)*, IEEE, May 2025, pp. 1–7. doi: 10.1109/GINOTECH63460.2025.11076673.

[41] S. Garg, "Predictive Analytics and Auto Remediation using Artificial Inteligence and Machine learning in Cloud Computing Operations," *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci.*, vol. 7, no. 2, 2019.

[42] M. R. R. Deva and N. Jain, "Utilizing Azure Automated Machine Learning and XGBoost for Predicting Cloud Resource Utilization in Enterprise Environments," in *2025 International Conference on Networks and Cryptology (NETCRYPT)*, IEEE, May 2025, pp. 535–540. doi: 10.1109/NETCRYPT65877.2025.11102235.

[43] D. Patel, "Zero Trust and DevSecOps in Cloud-Native Environments with Security Frameworks and Best Practices," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, 2023.

[44] H. Attou *et al.*, "Towards an Intelligent Intrusion Detection System to Detect Malicious Activities in Cloud Computing," *Appl. Sci.*, vol. 13, no. 17, p. 9588, Aug. 2023, doi: 10.3390/app13179588.

[45] A. Isong, B. U. Stephen, P. Asuquo, C. Ihemereze, and I. Enang, "Machine Learning Based Cloud Computing Intrusion Detection," *Adv. Inf. Syst.*, vol. 10, no. 1, pp. 115–125, Jan. 2026, doi: 10.20998/2522-9052.2026.1.13.

[46] A. Alshammari and A. Aldribi, "Apply machine learning techniques to detect malicious network traffic in cloud computing," *J. Big Data*, vol. 8, no. 1, p. 90, Dec. 2021, doi: 10.1186/s40537-021-00475-1.

[47] P. O. Prakash, K. Sasirekha, and D. Vistro, "A DDOS prevention system designed using machine learning for cloud computing environment," *Int. J. Manag.*, vol. 11, no. 10, pp. 1797–1806, 2020, doi: 10.34218/IJM.11.10.2020.167.